PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	)	Confirmation No. 2863
	)	
Johnson	)	Group Art Unit: 2137
	)	
Serial No.: 10/085,895	)	Examiner: Pearson, David J.
	)	
Filed: February 28, 2002	)	HP Docket: 10017900-1
	)	TKHR Docket: 50830-1430
	)	
For: **System and Method for Authenticating**	)	
Session and Other Transactions	)	

SUBSTITUTE APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Brief - Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This is an appeal from the decision of Examiner David Pearson, Group Art Unit 2137, mailed October 12, 2006, rejecting claims 1-28 of the present application and making the rejection FINAL.

I. REAL PARTY IN INTEREST

The real party in interest of the instant application is Hewlett-Packard Development Company, a Texas Limited Liability Partnership having its principal place of business in Houston, Texas.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF THE CLAIMS

Claim 1-28 are pending in this application, and all claims were rejected by the FINAL Office Action and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

There have been no claim amendments made after the Final Office Action, and all amendments made before the Final Office Action have been entered. Therefore, all claims 1-28 remain pending in their original form. A copy of the current claims is attached hereto as Appendix A.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the claimed subject matter are illustrated in FIGs. 2 through 9 and are discussed in the specification at least at pages 14-30.

Embodiments of the invention, such as those defined by claim 1, define a method for authenticating a Web session (see e.g., FIG. 3 and related description) comprising: receiving a user ID (see e.g., reference number 210 and related description, including p. 17, lines 1-4); computing a message digest of the user ID (see e.g., reference number 215 and related description, including p. 17, lines 6-11); computing an expiration timestamp for the session (see e.g., reference number 220 and related description, including p. 17, line 11 through p. 18, line 9); selecting an index number (see e.g., reference number 225 and related description, including p. 18, lines 10-11); combining the message digest and expiration timestamp (see e.g., reference number 230 and related description, including p. 18, lines 12-14); accessing an encryption key using the index number (see e.g., reference number 235 and related description, including p. 18, line 15 through p. 19, line 9); encrypting the combined message using the accessed encryption key (see e.g., reference number 240 and related description, including p. 19, lines 10-13); and converting the encrypted message into an ASCII string (see e.g., reference number 245 and related description, including p. 19, lines 13-21).

Embodiments of the invention, such as those defined by claim 9, further define the method of claim 1, wherein the step of encrypting the combined message (see e.g., reference number 240 and related description, including p. 19, lines 10-13) more specifically comprises encrypting the combined message digest and timestamp into an eight-byte binary value (see e.g., page 20, line 20).

Embodiments of the invention, such as those defined by claim 17, define a system for authenticating a transaction (see e.g., FIG. 5 and related description, including p. 24, line 19 through p. 25, line 12) comprising: logic configured to receive a user ID (see e.g., reference number 151 and related description, including p. 25, lines 1-2); logic configured to compute a message digest of the user ID (see e.g., reference number 152 and related description, including p. 25, lines 2-4); logic configured to select an index number (see e.g., reference number 154 and related description, including p. 25, lines 4-6); logic configured to combine the message digest with expiration timestamp (see e.g., reference number 155 and related description, including p. 25, line 6); logic configured to select an encryption key from a plurality of encryption keys using the index number (see e.g., reference number 156 and related description, including p. 25, lines 8-9); logic configured to encrypt the combined message using the selected encryption key (see e.g., reference number 157 and related description, including p. 25, lines 12-13); and logic configured to convert the encrypted message into an ASCII string (see e.g., reference number 158 and related description, including p. 25, lines 15-16).

Embodiments of the invention, such as those defined by claim 21, define a method for authenticating a transaction (see e.g., FIG. 6 and related description, including p. 26, lines 3-12) comprising: computing a message digest of a user ID (see e.g., reference number 215 and related description, including p. 17, lines 6-11); concatenating the message digest with an expiration timestamp (see e.g., reference number 315 and related description, including p. 26, lines 5-6); selecting an index number (see e.g., reference number 325 and related description, including p. 26, lines 6-7); selecting an encryption key from a plurality of encryption keys using the index number (see e.g., reference number 335 and related description, including p. 26, lines 7-8); encrypting the message digest using the selected encryption key (see e.g., reference number 340 and related description, including p. 26, lines 8-9); and converting the encrypted message into an ASCII string (see e.g., reference number 345 and related description, including p. 26, lines 10-12).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The FINAL Office Action rejected claims 1-2, 4, 8, 11-12, 17-20, and 21-24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Shrader et al. (U.S. Patent 6,374,359), and further in view of Rail (Patent Application Publication 2003/00110399), Serbinis et al. (U.S. Patent 6,314,425) and Garrison (U.S. Patent 6,275,939).

The Office Action rejected claim 9 under 35 U.S.C. § 103(a) as allegedly unpatentable over Shrader, Rail, Serbinis, and Garrison as applied to claim 1, and further in view of Jenkins ("A Hash Function for Hash Table Look-up") and Krishnaswamy (U.S. Patent 6,909,708).

VII. ARGUMENT

Claim 1-28 are pending in the present application, and all claims stand rejected under 103 for various combinations of cited references. For at least the reasons set forth below, Applicant respectfully traverses these rejections.

Discussion of rejection of claims 1-2, 4, 8, 11-12, 17-20, and 21-24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Shrader et al., and further in view of Rail, Serbinis et al., and Garrison

Independent claims 1, 17, and 21

The present application contains three independent claims: claims 1, 17, and 21. The Office Action has rejected each of these claims under 35 U.S.C. § 103(a) as allegedly unpatentable over the combination of U.S. patent 6,374,359, and further in view of U.S. published application 2003/0110399 to Rail, Serbinis et al. (U.S. Patent

6,314,425), and Garrison (U.S. Patent 6,275,939). For at least the following reasons, Applicant disagrees.

No proper reason or motivation to combine

For each of claims 1, 17, and 21, the FINAL Office Action:

1. admitted that Shrader does not teach computing a message digest of the user ID, but alleged that Rail teaches this at paragraph [0036]; (Office Action, pp. 3, 7, and 10);
2. admitted that the combination of Shrader and Rail fail to specify computing an expiration timestamp for the session and combining the message digest and expiration timestamp, but alleged that Serbinis teaches this at col. 21, lines 1-10 (Office Action, pp. 3, 7, and 10-11); and
3. admitted that the combination of Shrader, Rail, and Serbinis fail to specify selecting an index number, accessing an encryption key using the index number, and encrypting the message using the accessed encryption key, but alleged that Garrison teaches this at col. 6, lines 33-36 and col. 5, lines 61-65 (Office Action, p. 4, 8, and 11).

In each instance, the Office Action went on to allege that the combination of these references would have been obvious. Specifically, the Office Action alleged that the combination of Rail with Shrader would have been obvious "because the message digest would provide integrity." The Office Action alleged that the further combination of Serbinis would have been obvious "because an expiration timestamp would limit the re-use of a stolen message digest." Finally, the Office Action alleged that the further combination of Garrison would have been obvious "because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack."

These rejections embody the quintessential hindsight reasoning that the legal precedent surrounding 35 U.S.C. § 103(a) is intended to prevent. In each instance of combining the teachings of an additional reference, the rationale espoused by the Examiner merely reflected a perceived benefit (e.g., utilitarian) to the additional element. Under this approach, ANY claim submitted for examination could always be rejected. In this regard, it has long been stated that every patent claim is merely a novel combination of known elements. Therefore, by definition, every individual element of a patent claim can be found in the prior art. If it was sufficient to merely recited some utilitarian benefit that results when certain elements are combined, then any claim could be rejected.

To make the present rejection even more tenuous, the Examiner has relied on piecemeal teachings of four different references that are collectively required to reject the independent claims. In this regard, the rationale espoused by the Office Action is both incomplete and improper in view of the established standards for rejections under 35 U.S.C. § 103.

In this regard, the MPEP section 2141 states:

> Office policy has consistently been to follow Graham v. John Deere Co. in the consideration and determination of obviousness under 35 U.S.C. 103. As quoted above, the four factual inquires enunciated therein as a background for determining obviousness are briefly as

> follows:
>
> (A) Determining of the scope and contents of the prior art;
>
> (B) Ascertaining the differences between the prior art and the claims in issue;
>
> (C) Resolving the level of ordinary skill in the pertinent art; and
>
> (D) Evaluating evidence of secondary considerations.
>
> . . .
>
> BASIC CONSIDERATIONS WHICH APPLY TO OBVIOUSNESS REJECTIONS
>
> When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to:
>
> (A) The claimed invention must be considered as a whole;
>
> (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;
>
> (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention and
>
> (D) Reasonable expectation of success is the standard with which obviousness is determined.
>
> Hodosh v. Block Drug Co., Inc., 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986).

Simply stated, the Office Action has failed to at least (1) ascertain the differences between and prior art and the claims in issue; and (2) resolve the level of ordinary skill in the art. Furthermore, the alleged rationales for combining the four references (i.e., “because the message digest would provide integrity”, “because an expiration timestamp would limit the re-use of a stolen message digest”, and “because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack”) embodies clear and improper hindsight rationale. For at least this reason, the rejections of independent claims 1, 17, and 21 should be overturned.

As a separate and independent basis for the overturning of the rejections of claims 1, 17, and 21, the undersigned respectfully submits that the cited art does not teach what the Office Action alleged that it teaches (and relied on in order to reject the claims). For example, the Office Action applied col. 21, lines 1-10 of Serbinis for allegedly teaching the computation of an expiration timestamp and the combining of the timestamp with a message digest.

This cited portion of Serbinis actually states:

> At step 235, ***server computer 20 generates two random strings of alphanumeric data, T and K***.
>
> At step 237, ***server computer 20 generates an access token by: (1) concatenating an expiry timestamp for the access token*** (or a timestamp token from a timestamping authority) (TST) ***to T resulting in T+TST***; (2) hashing K using a well-known hashing algorithm such as MD5 (described in RFC (Request for Comments) 1321) resulting in H(K); (3) using a known symmetric encryption algorithm to encrypt T+TST with H(K) resulting in a message authentication code (MAC); and (4) concatenating T+TST+MAC, where T, TST and MAC are all of known lengths. Server computer 20 then uses the access token to generate a URL:

As set forth in this cited portion of Serbinis, Serbinis teaches concatenating an expiry timestamp with "T", which is taught to be a random string. In contrast, claim 1 defines "combining the message digest and expiration timestamp." Claim 1 further defines that the message digest is a compute value of the user's ID (and not merely a random number). Accordingly, even if Serbinis could be properly combined with Shrader and Rail, the resulting combination would not disclose the features of claim 1. For at least this additional reason, the rejection of claim 1 should be overturned.

Similar to claim 1 in this regard, independent claim 17 recites: “logic configured to combine the message digest with expiration timestamp.” As set forth above, Serbinis does not teach the combination of a “message digest” with an expiration timestamp. Therefore, even if Serbinis could be properly combined with Shrader and Rail, the resulting combination would not disclose the features of claim 17.

Similarly, independent claim 21 recites: “concatenating the message digest with an expiration timestamp.” As set forth above, Serbinis does not teach the combination of a “message digest” with an expiration timestamp. Therefore, even if Serbinis could be properly combined with Shrader and Rail, the resulting combination would not disclose the features of claim 21.

Another reason for overturning the rejections of claim 1, 17, and 21, relates to the applied teaching of Rail. The Office Action alleged that “Rail teaches computing a message digest of the user ID” in paragraph [0036]. This paragraph of Rail actually teaches:

> [0036] At step 416, passkey 214 is created. In one embodiment, passkey 214 is created as follows. Network identification 504, IP address 506, and time stamp 508 is temporarily stored in a buffer (not shown) as a string of data fields. Network identification 504 is known because it is input by the user and verified by ID and password validation tool 222. IP address 506 is known because it is unique to a particular client 106. Time stamp 508 is determined by authentication server 110 based on the current time. CRC 502 is then determined for the string of data fields using any suitable algorithm stored in authorization passkey creation tool 224. The string of data fields is appended with CRC 502 before length 500 is determined for the string of data fields. Length 500 is then appended to the string of data fields to create passkey 214. Other suitable methods of creating passkey 214 may be utilized. Length 500 may be determined on the string of data fields containing network identification 504, IP address 506, and time

> stamp 508. In other embodiments, length 500 is determined on a string of data fields containing network identification 504, IP address 506, time stamp 508, and CRC 502. Passkey creation tool 224 uses any suitable encryption technique to encrypt passkey 214. In one embodiment, an 80 bit encryption technique is utilized.

The present application teaches that a “message digest” is simply a binary number that is representative of the user ID. In this regard, the message digest may be a simple checksum or other processed value. In the illustrated embodiment, the message digest is four bytes in length. Therefore, the system converts the user ID into a four-byte binary value. (present application, p. 17, lines 7-11). Simply stated, Rail does not teach the claimed feature of “computing a message digest of the user ID” as recited in claim 1.

Independent claims 17 and 21 similarly recite: “logic configured to compute a message digest of the user ID” and “computing a message digest of a user ID.” Therefore, for reasons similar to those expressed above in connection with claim 1, Rail fails to disclose at least these recited elements of claims 17 and 21. For at least these additional reasons, the rejections of independent claims 1, 17, and 21 should be overturned.

Dependent Claims

Claims 2-16, 18-20, and 22-28 depend from independent claims 1, 17, and 21, respectively and the rejections of these claims should be overturned for at least the reasons set forth above in connection with claims 1, 17, and 21.

Discussion of rejection of claim 9 under 35 U.S.C. § 103(a) as allegedly unpatentable over Shrader, Rail, Serbinis, and Garrison as applied to claim 1, and further in view of Jenkins and Krishnaswamy

In addition, Applicant further submits that the rejection of dependent claim 9 is misplaced. In this regard, the Office Action rejected claim 9 under 35 U.S.C. § 103(a) as allegedly unpatentable over Shrader, Rail, Serbinis, and Garrison as applied to claim 1, and further in view of Jenkins and Krishnaswamy.

Claim 9 recites:

> 9. The method of claim 1, wherein the step of encrypting the combined message more specifically comprises encrypting the combined message digest and timestamp into an eight-byte binary value.

In citing Jenkins, the Office Action states that Jenkins discloses a four-byte value, and that Jenkins "teaches his hash function is 'faster and more thorough than the one you are using now.'" (Office Action, p. 18). As claim 9 recites encrypting the combined message digest and timestamp into an eight-byte binary value, the undesigned fails to understand the relevance of the four-byte value allegedly taught by Jenkins. Further, claim 9 teaches nothing about a "hash" function, so there seems to be no relevance to the statement that Jenkins' "hash function" is "more thorough." Simply stated, this rejection seems to be completely misplaced with respect to the claimed embodiment and the rejection of claim 9 should be overturned for this independent reason.

CONCLUSION

Based upon the foregoing discussion, Applicant respectfully requests that the Examiner's final rejection of claims 1-28 be overturned by the Board.

In addition to the claims of Appendix A, Appendix B attached hereto indicates that there is no evidence being attached and relied upon by this brief. Appendix C attached hereto indicates that there are no related proceedings.

Please charge Hewlett-Packard Company's deposit account 08-2025 in the amount of $500 for the filing of this Substitute Appeal Brief. No additional fees are believed to be due in connection with this Appeal Brief. If, however, any additional fees are deemed to be payable, you are hereby authorized to charge any such fees to deposit account No. 08-2025.

Respectfully submitted,

/Daniel R. McClure/

Daniel R. McClure
Registration No. 38,962

(770) 933-9500

VIII. CLAIMS - APPENDIX

1. A method for authenticating a Web session comprising:

receiving a user ID;

computing a message digest of the user ID;

computing an expiration timestamp for the session;

selecting an index number;

combining the message digest and expiration timestamp;

accessing an encryption key using the index number;

encrypting the combined message using the accessed encryption key; and

converting the encrypted message into an ASCII string.

2. The method of claim 1, wherein the step of combining the message digest and expiration timestamp more specifically includes concatenating the message digest and expiration timestamp.

3. The method of claim 1, further comprises passing the ASCII string to a remote computer using an FTP (file transport protocol) URL (uniform resource locator) within an HTML (hyper-text markup language) page, the FTP URL being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

4. The method of claim 1, wherein the step of receiving the user ID more specifically comprises receiving the user ID through an HTML (hyper-text markup language) page that is communicated from a remote client browser.

5. The method of claim 1, wherein the step of computing a message digest of the user ID more specifically comprises computing a four-byte binary value which is an encoded form of the user ID.

6. The method of claim 1, wherein the step of computing an expiration timestamp more specifically comprises computing an expiration timestamp in Epoch format.

7. The method of claim 1, wherein the step of selecting an index number more specifically comprises generating a random number within a predefined range of values.

8. The method of claim 1, wherein the step of accessing the encryption key more specifically comprises retrieving an encryption key from a storage segment containing a plurality of encryption keys, wherein the retrieved encryption key is obtained from a location or position within the storage segment based upon the index number.

9. The method of claim 1, wherein the step of encrypting the combined message more specifically comprises encrypting the combined message digest and timestamp into an eight-byte binary value.

10. The method of claim 1, further comprising the step of concatenating the index number to the encrypted message.

11. The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically comprises using a "printf" command.

12. The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value.

13. The method of claim 10, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting the encrypted message and the index number into an ASCII string using a "printf" command.

14. The method of claim 3, further including the step of passing the index number to the remote computer.

15. The method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string.

16. The method of claim 14, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting a combination of the encrypted message and the index number into an ASCII string, wherein the index number is communicated to the remote computer as a part of the ASCII string.

17. A system for authenticating a transaction comprising:

logic configured to receive a user ID;

logic configured to compute a message digest of the user ID;

logic configured to select an index number;

logic configured to combine the message digest with expiration timestamp;

logic configured to select an encryption key from a plurality of encryption keys using the index number;

logic configured to encrypt the combined message using the selected encryption key; and

logic configured to convert the encrypted message into an ASCII string.

18. The system of claim 17, further including logic configured to generate an expiration timestamp.

19. The system of claim 17, further including logic configured to communicate the ASCII string to a remote computer.

20. The system of claim 17, further including a local memory for storing the plurality of encryption keys.

21. A method for authenticating a transaction comprising:

computing a message digest of a user ID;

concatenating the message digest with an expiration timestamp;

selecting an index number;

selecting an encryption key from a plurality of encryption keys using the index number;

encrypting the message digest using the selected encryption key; and

converting the encrypted message into an ASCII string.

22. The method of claim 21, wherein the step of encrypting the message more specifically includes encrypting the concatenated message using the accessed encryption key.

23. The method of claim 21, wherein the step of selecting the encryption key more specifically includes retrieving the encryption key from a local memory based on the index number.

24. The method of claim 21, further including the step of communicating the ASCII string to a remote computer.

25. The method of claim 21, further including the step of communicating the ASCII string to a person through voice communication.

26. The method of claim 21, further including the step of printing the ASCII string onto a ticket.

27. The method of claim 26, wherein the ticket is one selected from the group consisting of an airline ticket, a concert ticket, an employee ID card, and an event ticket.

28. The method of claim 26, wherein the step of printing the ASCII string onto a ticket more specifically includes printing the ASCII string onto the ticket in a form that it may be later electronically scanned for verification.

IX. EVIDENCE - APPENDIX

None.

IX. RELATED PROCEEDINGS- APPENDIX

None.